

FIG. 1A

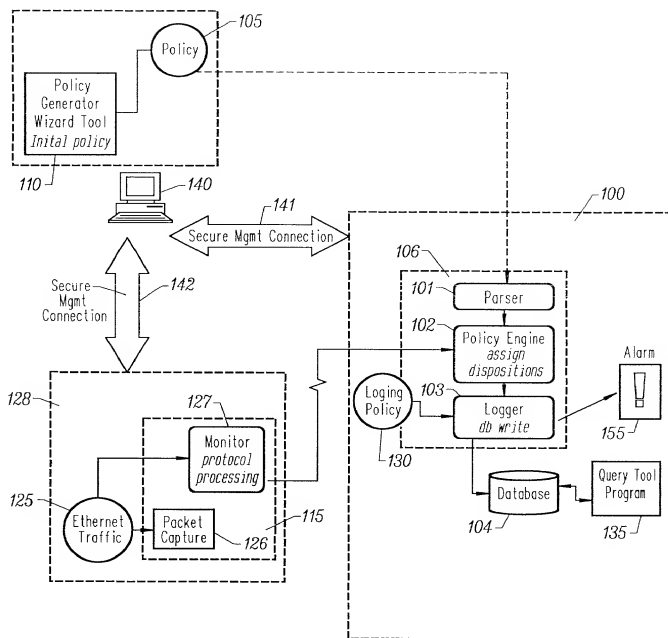


FIG. 1B

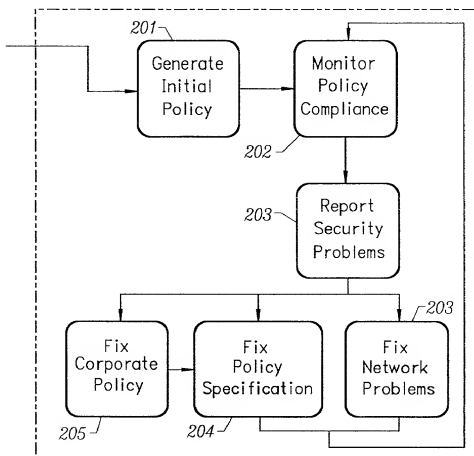


FIG. 2

301

K Policy Generator

File Help

☐ ☐ ☐ ☐

Community	Policy Domains	Rules	Service
Name	Includes	Excludes	Description
Inside_Nodes	10.0.0.0/8		The Hosts in out Intranet <input type="checkbox"/>
Outside_Nodes		Inside_Nodes	All hosts in the Intranet <input type="checkbox"/>

☐ New

FIG. 3

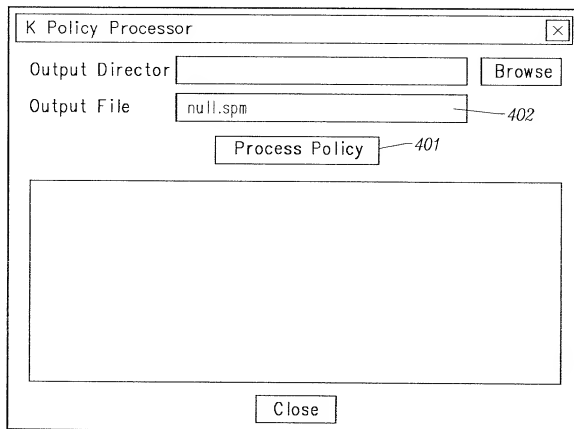


FIG. 4A

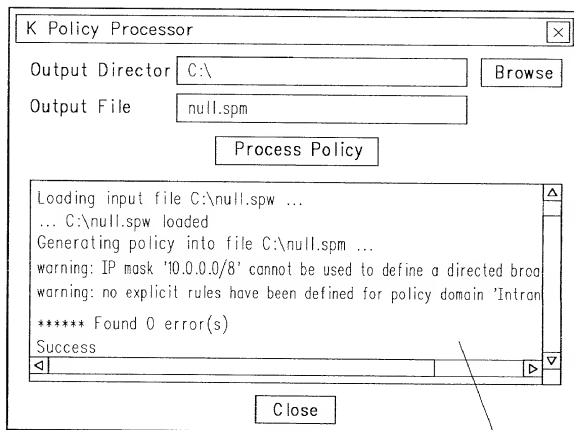


FIG. 4B

PM:50: 04:22:00

SPM: Argument Selector Dialog

Monitor configuration

Input dump file: C:\qs.dmp 501 Browse

Policy: C:\null.spm 502 Browse

Monitoring Point: INTRANET\_MONITOR 503  
(comma separated)

Run 507

Exit

Advanced

Help

Progress

nPkts

100%

0%

Monitor Logging Options

Execution Run Comment:

ODBC name: sybase 504

DB Username: policy 505

DB Password: \*\*\*\*\* 506 ☒ Save Password [insecure]

Output Options

☐ Output to console:

☒ Output to file: C:\output.txt

Browse

FIG. 5

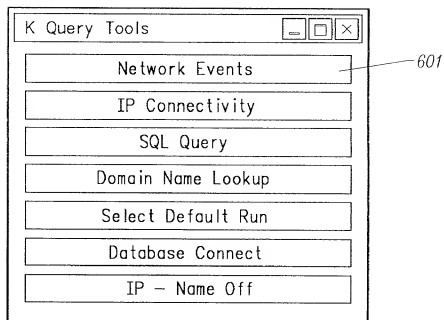


FIG. 6

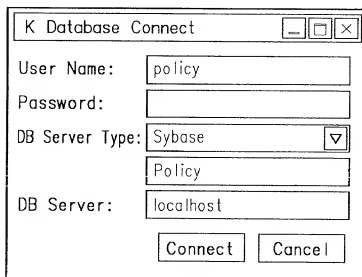


FIG. 7



K Rule View		X	
Execution Run:		1999-10-01 14:30:20.0 C:\.bmp	
Final Rule Name:		<Any Rule>	
Disposition Name:		<Any Disposition>	
Disposition Codes: <input type="checkbox"/> Access Denied <input type="checkbox"/> Auth Violation <input type="checkbox"/> Security Attack <input type="checkbox"/> Security QOS <input type="checkbox"/> Policy Error <input type="checkbox"/> OK			
Disposition Severity: <input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Monitor <input type="checkbox"/> Warning <input type="checkbox"/> Information <input type="checkbox"/> <none>			
Query			
Rows			
Done		Edit SQL	Copy Row
		Copy Deep	

FIG. 8

K Rule View		X				
Execution Run:		1999-10-01 14:30:20.0 C:\.bmp				
Final Rule Name:		<Any Rule>				
Disposition Name:		<Any Disposition>				
Disposition Codes:		<input type="checkbox"/> Access Denied <input type="checkbox"/> Auth Violation <input type="checkbox"/> Security Attack <input type="checkbox"/> Security QOS <input type="checkbox"/> Policy Error <input type="checkbox"/> OK				
Disposition Severity:		<input type="checkbox"/> Critical <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Monitor <input type="checkbox"/> Warning <input type="checkbox"/> Information <input type="checkbox"/> <none>				
Query						
Rule Name	Disposition Name	Initiator IP	Init Name	Target IP	Targ Name	Targ Service
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.198		http
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.201		http
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.198		http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	204.71.200.68	www3.yahoo.com	http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.97	kabole.securify.com	http
Top_Missed_Connections	Warn_Missed_Tcp_Connect	10.5.63.143	vg-143.securify.com	10.5.63.24	Fred.securify.com	netbios-ssn
<div> <div>Rows 10</div> <div>Done</div> <div>Edit SQL</div> <div>Copy Row</div> <div>Copy Deep</div> </div>						

FIG. 9

K Policy Generator				<input type="button" value="-"/> <input type="button" value="X"/>	
File Help					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Community	Policy Domains	Rules	Service		
-Select Policy Domain: Policy Domain: <input type="text" value="Intranet"/>					
-Identify New or Existing Rule in Intranet			Rule Name: <input type="text" value="Internal_Dns"/> <input type="button" value="X"/> <input type="button" value="Delete"/>		
Add Elements to Internal_Dns			<input type="button" value="Set"/>		
Initiators:		Services:		Targets:	
<input type="text" value="Intranet =="/> Inside_Nodes ... Firewall ... Outside_Nodes		AUTH BOOTP_CLIENT BOOTP_SERVER DNS FINGER		== Intranet == Inside_Nodes ... Firewall ... Outside_Nodes	
<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>	
Rule Contents for Internet* Dns					
Initiators:		Services:		Targets:	
<input type="text" value="&lt;Any&gt;"/>		<input type="text" value="&lt;Any&gt;"/>		<input type="text" value="&lt;Any&gt;"/>	
<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>	

K Policy Generator				<input type="button" value="F1"/> <input type="button" value="F2"/> <input type="button" value="F3"/> <input type="button" value="F4"/> <input type="button" value="F5"/> <input type="button" value="F6"/> <input type="button" value="F7"/> <input type="button" value="F8"/> <input type="button" value="F9"/> <input type="button" value="F10"/> <input type="button" value="F11"/> <input type="button" value="F12"/> <input type="button" value="Print"/> <input type="button" value="Exit"/>	
File Help					
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>					
Community		Policy Domains		Rules Service	
Select Policy Domain Policy Domain: <input type="text" value="Intranet"/> <input type="button" value="v"/>					
Identify New or Existing Rule in Intranet Rule Name: <input type="text" value="Internal_Dns"/> <input type="button" value="v"/> <input type="checkbox"/> New <input type="button" value="X"/> Delete					
Add Elements to Internal_Dns					
Description: Allow DNS to be served from any internal host <input type="button" value="Set"/>					
Initiators:		Services:		Targets:	
<input type="text" value="Intranet"/> <input type="text" value="Inside_Nodes"/> ... Firewall ... Outside_Nodes		<input type="text" value="AUTH"/> <input type="text" value="BOOTP_CLIENT"/> <input type="text" value="BOOTP_SERVER"/> <input type="text" value="DNS"/> FINGER		<input type="text" value="Intranet"/> <input type="text" value="Inside_Nodes"/> ... Firewall ... Outside_Nodes	
<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>	
Rule Contents for Internet* Dns					
Initiators:		Services:		Targets:	
<input type="text" value="Intranet"/> <input type="text" value="Inside_Nodes"/> ... Firewall ... Outside_Nodes		<input type="text" value="DNS"/>		<input type="text" value="Inside_Nodes"/>	
<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>		<input type="button" value="Add Selected"/>	

FIG. 10B

K Policy Generator				<input type="button" value="-"/> <input type="button" value="X"/>	
File Help					
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>					
Community	Policy Domains	Rules	Service		
Name	Includes	Excludes	Description		
Inside_Nodes	10.0.0.0/8		The Hosts in out Intranet <input type="checkbox"/>		
Outside_Nodes		Inside_Nodes	All hosts in the Intranet <input type="checkbox"/>		
<input type="checkbox"/> New			<input type="button" value="X"/> Delete		<input type="button" value="Find Uses"/>

FIG. 10C

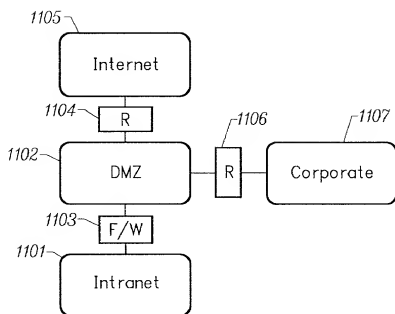


FIG. 11

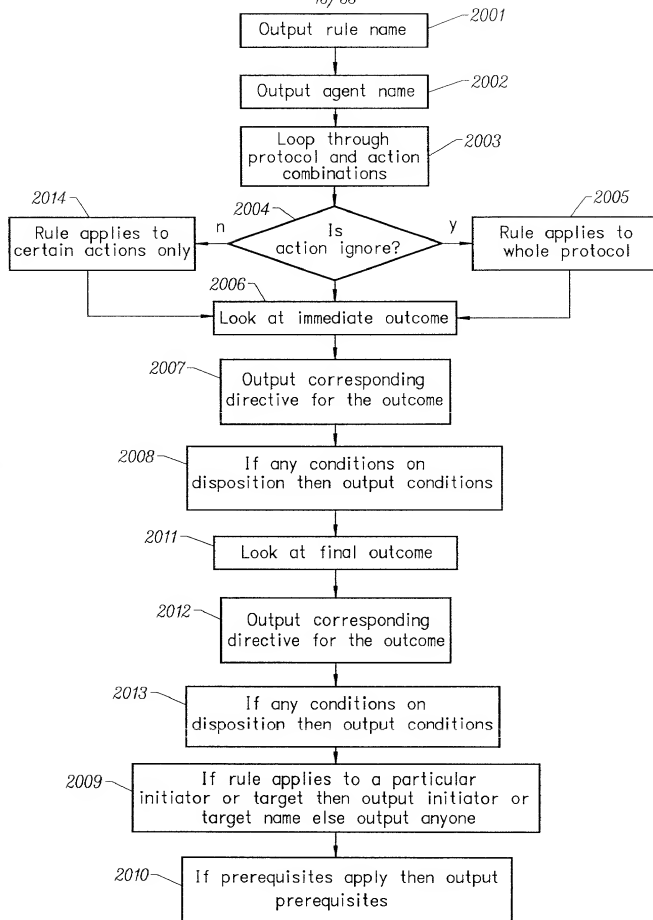


FIG. 12

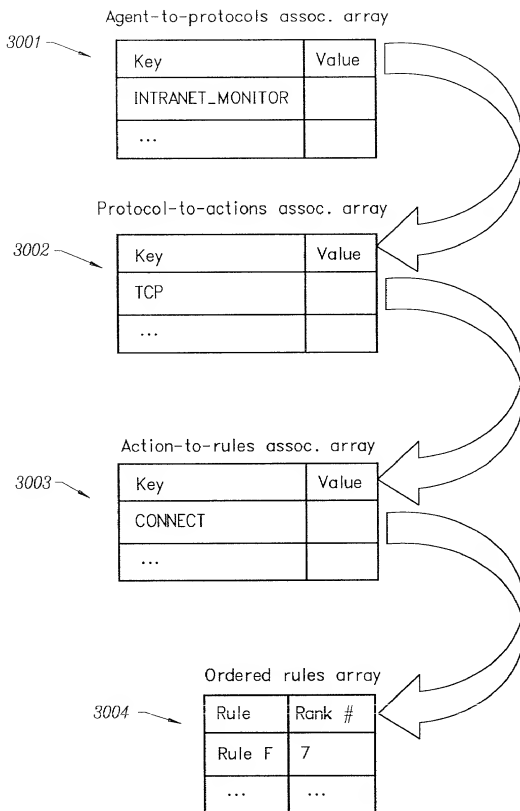


FIG. 13



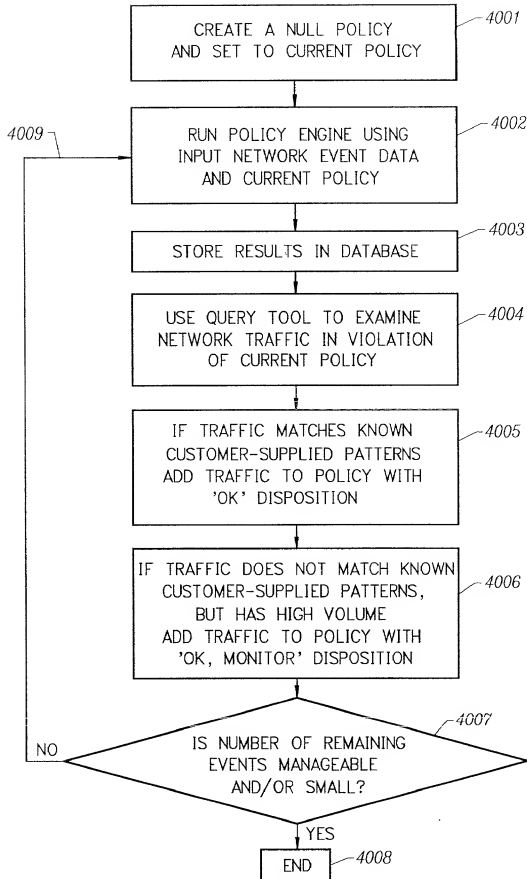


FIG. 14

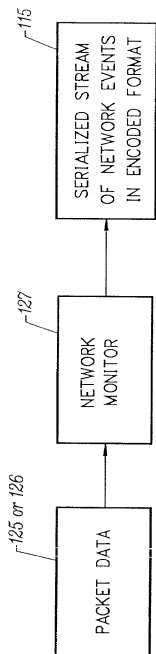


FIG. 15

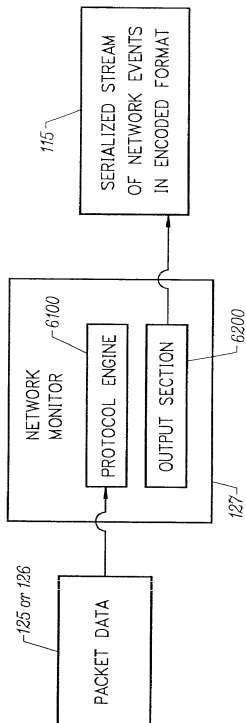


FIG. 16

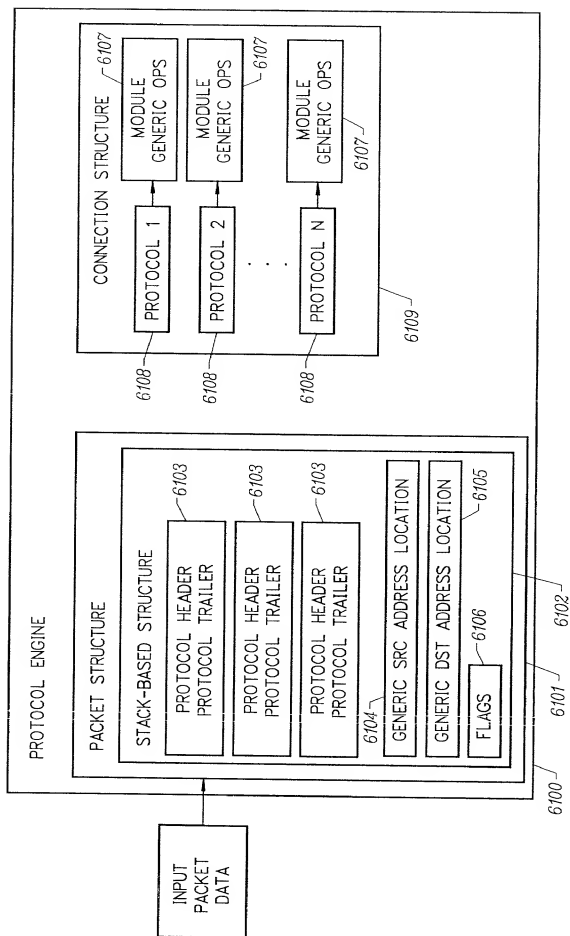


FIG. 17

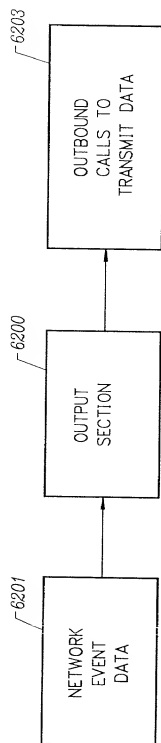


FIG. 18

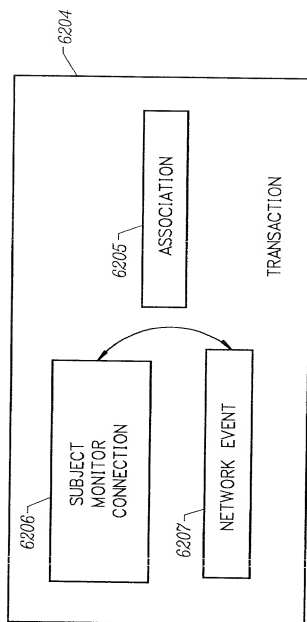
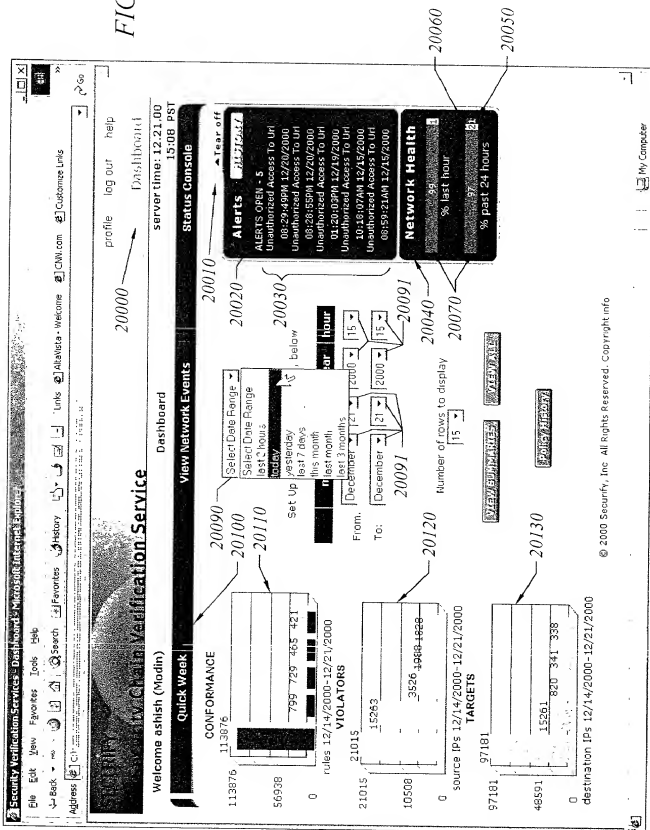


FIG. 19

FIG. 20



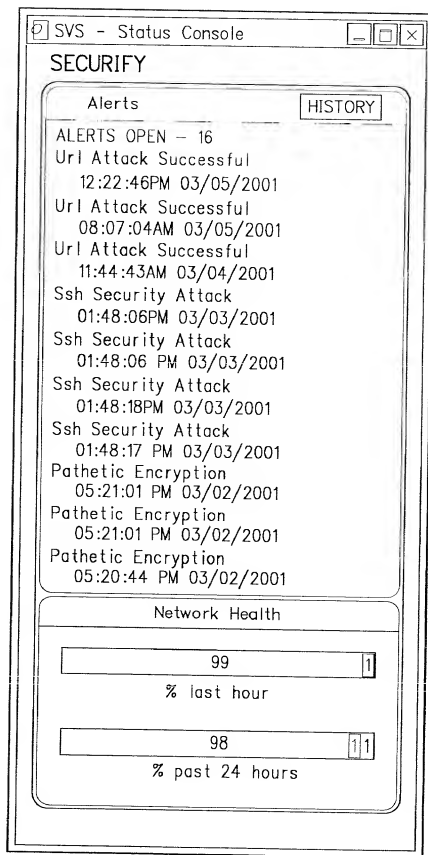


FIG. 21

FIG. 22

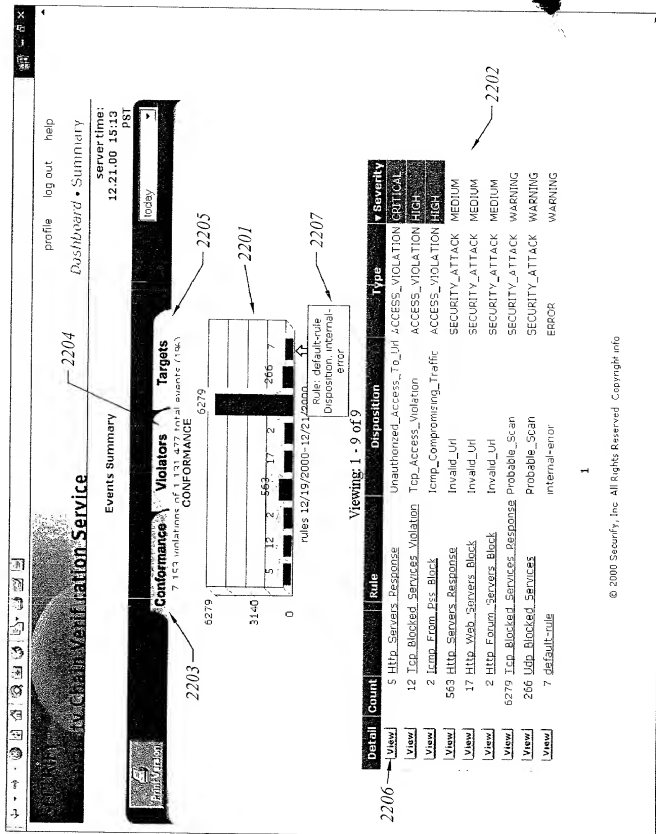
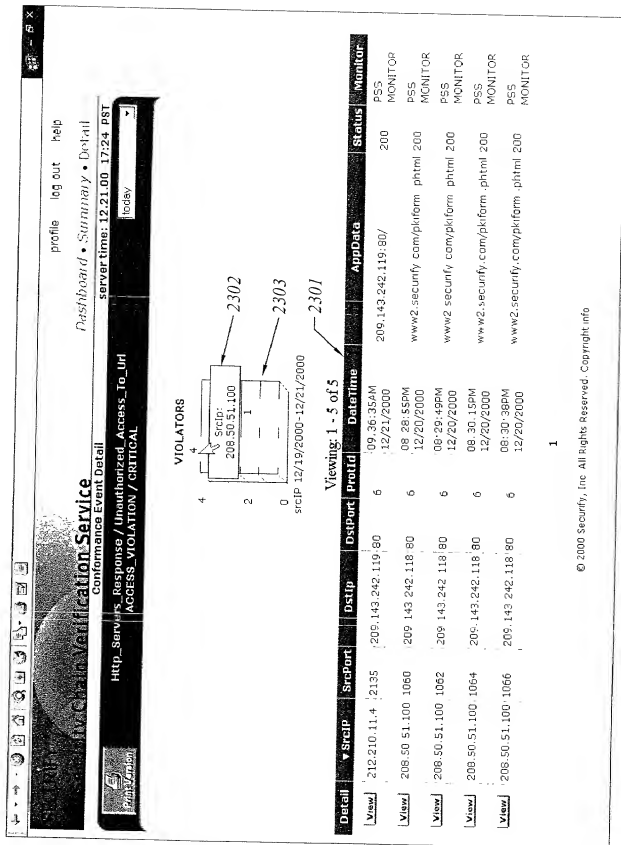


FIG. 23





profile log out help

*Dashboard • Policy History*

server time: 12.26.00 9:21 PST

Protocol Event Details

[HTTP Servers\\_Response / Unauthorized Access\\_To Url](#)  
**ACCESS\_VIOLATION / CRITICAL**

Select Protocol - Action

- > IP ASSOCIATION
- TCP-CONNECT
- HTTP-GET
- HTTP-RESPONSE
- TCP-CLOSE

IP - ASSOCIATION	
Protocol	Initiator Target
IPAddr32	212.210.11.4 209.143.242.119
Port	2135 80
IPAddr	0003326D83C00000 0050DA14E7C0000
IPProtid	6 6

© 2000 Security, Inc. All Rights Reserved. Copyright info

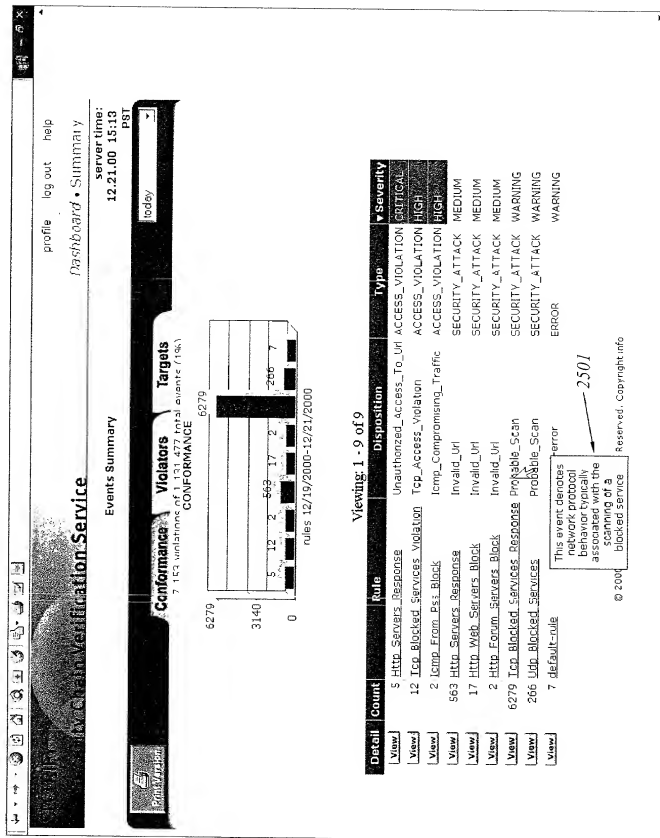
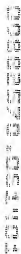


FIG. 25



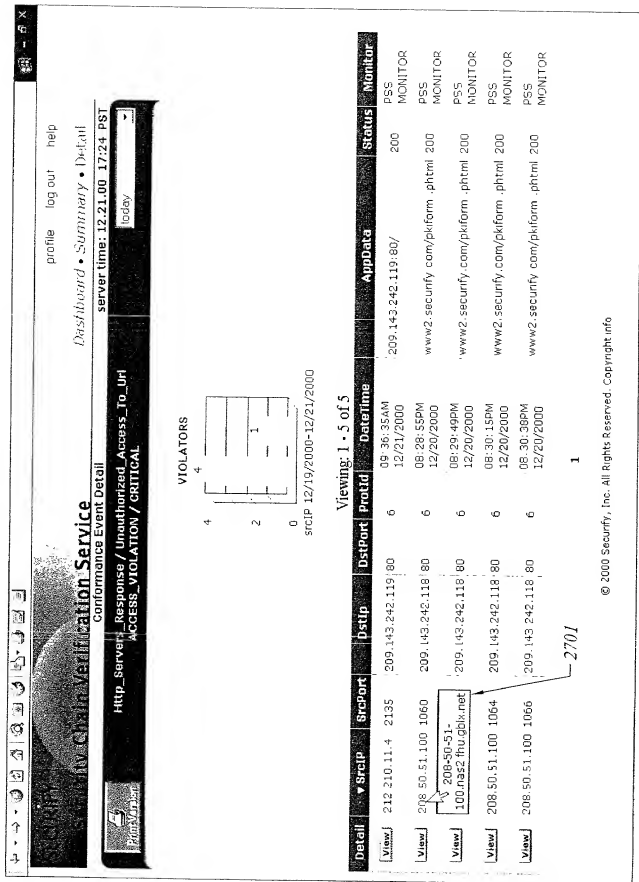


FIG. 27

29/33

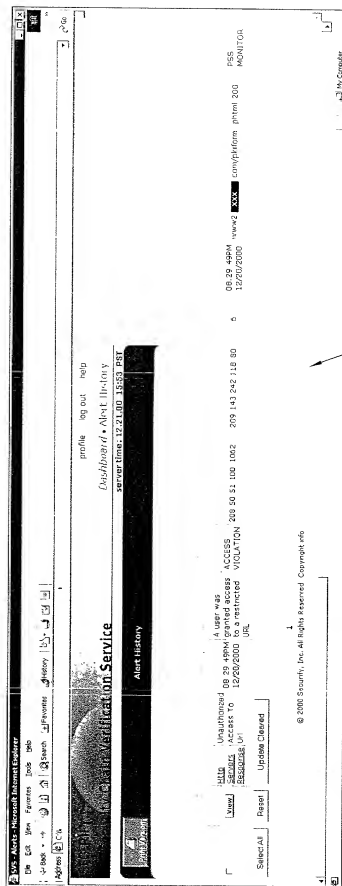


FIG. 28

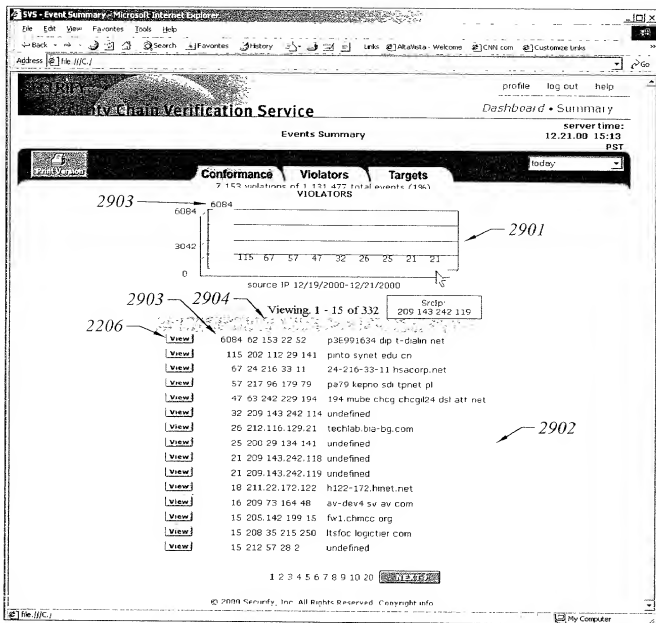


FIG. 29

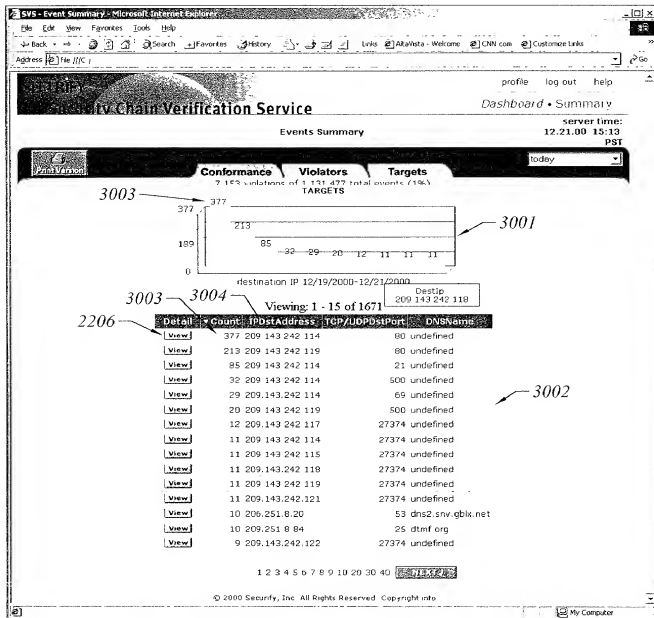


FIG. 30

Advanced Search - Microsoft Internet Explorer  
Address  Go

## SECURIFY

**Advanced Search** Close

Filter results by One or All of the following:

Protocol

Rule  3102

or   
(regular expression in Rule)

Disposition  3103

or   
(regular expression in Disposition)

Source IP  3106

Target IP

TargetPort

Monitor(s) 3106

All Monitors  
INTRANET\_LOCAL\_MONITOR  
INTRANET\_MONITOR  
PARTNER\_A\_MONITOR

© 2000, 2001 Securify, Inc. All Rights Reserved.  
Copyright info

*3101* points to the "Filter results by One or All of the following:" text.  
*3104* points to the "Rule" label.  
*3105* points to the "Disposition" label.  
*3106* points to the "Source IP" label.  
*3106* points to the "Monitor(s)" label.

FIG. 31



FIG. 32

